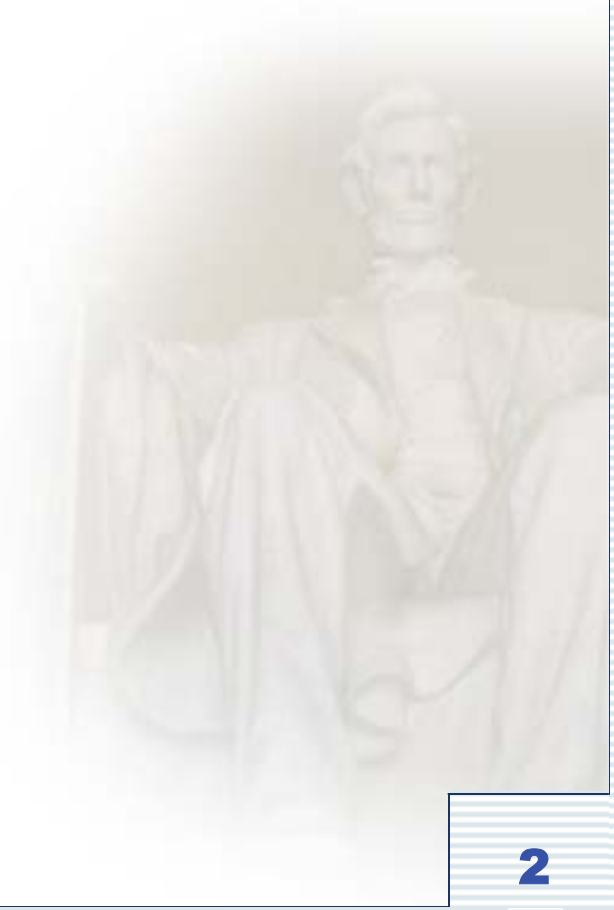
Wireless Security 101

Presented 03.04.2003 at the
Federal Information Systems Security Educators' Association
(FISSEA) conference

Agenda

- Introduction
- Agenda
- Goals
- Quiz
- Quiz Answers
- WLAN Productivity Case Study
- Overall Recommendations
- Goal Review
- References



Goals

- Become acquainted with basic wireless terminology
- Introduce basic wireless LAN equipment
- Address basic wireless LAN threats & vulnerabilities
- Discuss basic wireless LAN risk mitigation techniques
- Discuss wireless technology developments
- Discuss the future of wireless technology

Wireless 101

QUIZ

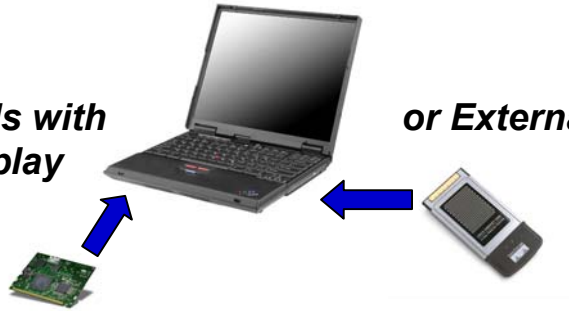
Why is it that the
only location **where**
employees have access
to all **their** productivity tools**...is the** one location
where they spend the
least **amount of time—**
their desks**?**

Question 1

What kinds of wireless communication devices do you use at work and/or at home?

a) Laptops, PDAs
b) Ham radios, CBs, Walkie Talkies
c) WLANs

By the end of 2003, 50% of All Corporate Laptops Will Have a WLAN Connection! -
Gartner/Dataquest, 9/02



Embedded Mini-PCI Cards with Antenna Built Into Display

or External PC Cards

Question 2

When did the first wireless message get sent?

a) When Marconi invented radio
b) When Cain hit Able with a piece of fruit
c) When smoke signals were seen off in the distance on the TV show Bonanza

Question 3

What does “wireless” communication mean?

a) Mobile access to information
b) Communication without wires
c) The transference of information without a physical transport medium

Question 4

What equipment comprises a basic wireless LAN?

a) Gateway, Server, Receiver, Laptop
b) Access Point, Client Network Interface Card, Laptop
c) Mobility Module, Firewall, Access Derivative, Laptop

Question 5

Which of the following most looks like a wireless Access Point?

a) 

b) 

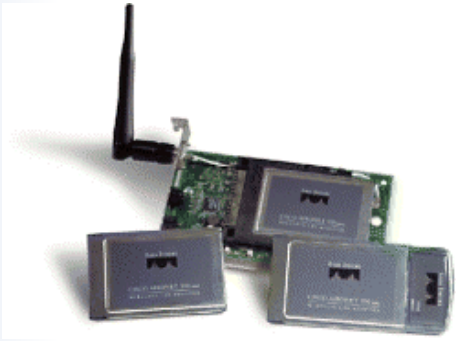
c) 

Question 6

Which of the following most looks like a wireless client Network Interface Card (NIC)?

a) 

b) 

c) 

Question 7

How does a basic wireless LAN work?

a) Access Points connected to the wired infrastructure broadcast radio waves that are picked up and connected to by client NICs
b) NICs receive signals from Access Points controlled by satellites
c) Access Points magically transmit stuff that laptops understand

Question 8

A wireless network's Service Set ID (SSID) is an identity-based verification mechanism that can be accessed by users who provide it with:

a) The proper shared cryptographic key
b) The proper network SSID
c) An empty string in place of the SSID

Question 9

Which of the following wireless standards are the most highly adopted and why?

a) 802.11a-5GHz, physical throughput of 54(30)Mbps, 8 Channels
b) 802.11b-Wireless Fidelity (Wi-Fi) 2.4GHz, 11(6)Mbps, 3 Channels, Lower Cost, Lower Power (important for handhelds)
c) 802.11c-Bridging
d) 802.11d-Multiple Regulatory Domains (International Regions)
e) 802.11e-Quality of Service
f) 802.11f-Inter-Access Point Protocol (Roaming)
g) 802.11g-2.4GHz, 54Mbps (High throughput upgrade from 802.11b that is fully forward/backward compatible with 802.11b)
h) 802.11h-Dynamic Frequency Selection & Transmit Power Control
i) 802.11i-Security
j) 802.1x-Security: Extensible Authentication Protocol (EAP)

Question 10

What are the main differences between 802.11a, 802.11b, and 802.11g?

a) 802.11a is faster than 802.11b
b) 802.11b is cheaper, has a wider broadcast range, and is more widely adopted than 802.11a
c) 802.11g is a high throughput version of 802.11b that is fully forward/backward compatible with existing 802.11b implementations

Question 11

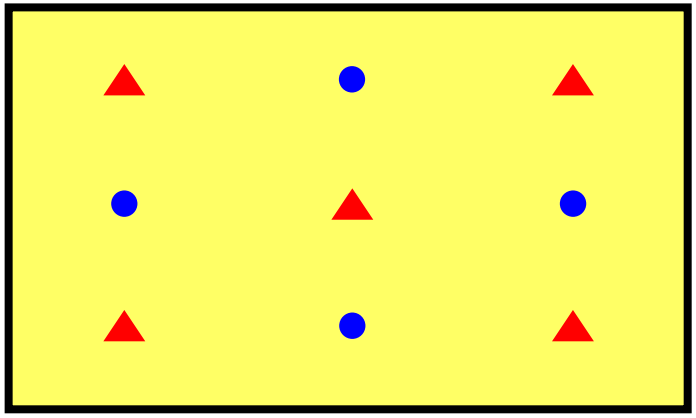
It can be a good idea to deploy both 802.11b & 802.11a Access Points (APs) together.

a) True
b) False

▲ = Dual-band coverage

● = 802.11a coverage

"802.11a Fill-in"

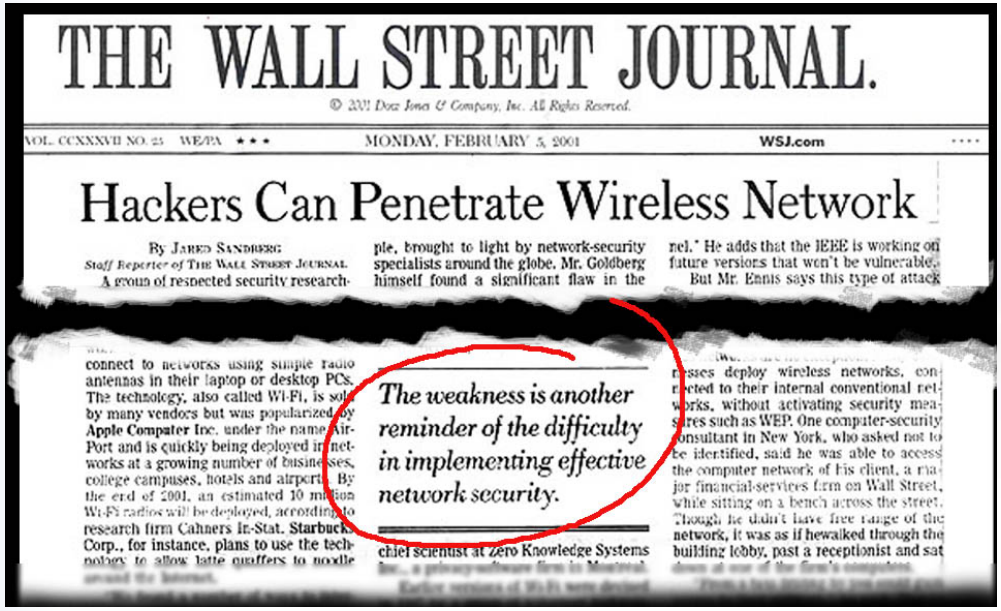


Deploy dual-band APs based on 802.11b coverage, then install 802.11a-only APs in between

Question 12

What are the biggest threats to a wireless LAN (WLAN)?

a) Theft of equipment
b) Unauthorized access
c) Acts by malicious users to include: Identity theft, loss of sensitive information, and connectivity to network management controls



THE WALL STREET JOURNAL.

© 2001 Dow Jones & Company, Inc. All Rights Reserved.

VOL. CCXXXVII NO. 25 WE/PA ★★★ MONDAY, FEBRUARY 5, 2001 WSJ.com

Hackers Can Penetrate Wireless Network

By JARED SANDBERG
Staff Reporter of THE WALL STREET JOURNAL

A group of respected security research-

ple, brought to light by network-security specialists around the globe. Mr. Goldberg himself found a significant flaw in the

nel." He adds that the IEEE is working on future versions that won't be vulnerable. But Mr. Ennis says this type of attack

connect to networks using simple radio antennas in their laptop or desktop PCs. The technology, also called Wi-Fi, is sold by many vendors but was popularized by Apple Computer Inc. under the name AirPort and is quickly being deployed in networks at a growing number of businesses, college campuses, hotels and airports. By the end of 2001, an estimated 10 million Wi-Fi radios will be deployed, according to research firm Cahners In-Stat. Starbucks Corp., for instance, plans to use the technology to allow latte quaffers to noodle around the Internet.

The weakness is another reminder of the difficulty in implementing effective network security.

chief scientist at Zero Knowledge Systems Inc., a privacy-software firm in Montreal.

sses deploy wireless networks, con- cted to their internal conventional net- works, without activating security mea- sures such as WEP. One computer-security consultant in New York, who asked not to be identified, said he was able to access the computer network of his client, a ma- jor financial-services firm on Wall Street, while sitting on a bench across the street. Though he didn't have free range of the network, it was as if he walked through the building lobby, past a receptionist and sat

Question 13

What are the biggest vulnerabilities of a WLAN?

a) Lack of physical security and standard default settings
b) All the vulnerabilities that exist in a conventional wired network
c) The inability to authenticate Access Points
d) Weak native encryption

Question 14

Which of the following provide wireless **authentication**?

a) 802.1x-based LEAP
b) 802.1x-based EAP-TLS
c) 802.1x-based PEAP with one-time passwords (OTP)

Question 15

The proper order of evolution in wireless **encryption** is:

a) WEP, TKIP, WPA, AES
b) AES, WPA, TKIP, WEP
c) LEAP, EAP-TLS, PEAP, AES

Level of Security	Encryption	Authentication
Bronze	**WEP**	**MAC**
Silver	**TKIP**	**LEAP**
Gold	**WPA**	**PEAP**
Platinum	**AES**	**PEAP + OTP**

Question 16

Which of the following are wireless intrusion detection tools?

a) NetStumbler Spyglass (NSS)
b) AirSnort
c) Internet Security Systems Wireless Scanner

Question 17

To mitigate WLAN risks one should:

a) Strategically place and tune Access Points (APs) so that wireless coverage is only available where needed
b) Have firewalling and router ACLs between the APs and the internal wired network
c) Use encryption between wireless nodes and wired nodes
d) Install Intrusion Detection tools on the wired side of the APs

Question 18

Wireless systems can provide inexpensive network redundancy.

a) True
b) False

"Properly designed, a wireless broadband network can be flexible, scalable, and customized enough to offer…solutions from a 'mirror image' voice/data 'hot standby' network to a single diverse private line connecting to a primary carrier."

Disaster Recovery Journal – Winter 2003

Question 19

Which of the following will help harden a wireless environment?

a) Aware Systems administrators, Managers, and End users
b) Changing the default SSID settings
c) Utilizing encryption methods

Question 20

The future of wireless is:

a) Imminent, since 802.11 technology has gone mainstream
b) Inexpensively increasing employee productivity
c) Likely to increase as Access Points extend wired networks
d) Important to understand in order to maintain availability, integrity, and confidentiality of information systems and their data

Quiz Answers

1. Group Participation
2. Group Participation
3. All
4. B
5. A, B
6. A, C
7. A
8. All
9. A, B, G,
10. All
11. It depends.
12. All
13. All
14. All
15. A
16. A, C
17. All
18. True
19. All
20. All

WLAN Case Study:
Increased Productivity at Microsoft

Campus-wide Cisco Aironet installation
+ Actively used by 40,000 employees
= 30 minute productivity gain per employee per day

- Minutes gained working at the beginning of slow starting meetings
- Eliminates “I’ll do it when I get back to my desk” syndrome
- Instant Messaging allows for getting answers without disturbing meetings
- Can send all participants (conf. call too) presentation so they can view it simultaneously without a projector

Overall Recommendations

- Allow “business needs” to determine implementations
- Ensure policies are established
- Ensure procedures are enforced
- Eliminate default passwords
- Despite their limited value, use the technical controls available (e.g. WEP)
- Identify devices with wireless functionality
- Utilize network discovery tools for Configuration Management (including discovery of rogue devices)
- Due to the frequency and complexity of changes in the wireless arena, ongoing education is vital

Goals

- Become acquainted with basic wireless terminology
- Introduce basic wireless LAN equipment
- Address basic wireless LAN threats & vulnerabilities
- Discuss basic wireless LAN risk mitigation techniques
- Discuss wireless technology developments
- Discuss the future of wireless technology

References

- NIST Special Publication 800-46, Wireless Network Security
- http://www.cisco.com/en/US/products/hw/wireless/index.html
- http://www.3com.com/products/en_US/prodlist.jsp?tab=cat&pathtype=purchase&cat=13&selcat=Wireless+Products
- http://www.netstumbler.com/
- http://airsnort.shmoo.com/
- http://home.attbi.com/~digitalmatrix/nsspyglass/

Thank you.

Falan Memmott
Department of Homeland Security
Federal Computer Incident Response Center
falan.memmott@gsa.gov